Claims

What is claimed is:

1. A method for obtaining status of public key certificate updates, the method comprising the steps of:

a) from time to time, providing public key certificate update subscription information to a server;

b) providing an indication of a local replica of current public key certificate to the server while on-line with the server;

c) receiving an indication of updated public key certificate from the serve when the updated public key certificate is inconsistent with the local replica of the current public key certificate; and

d) while on-line, receiving an indication of newly updated public key certificate from the server, wherein the newly updated public key certificate relates to information of interest as identified in the public key certificate update subscription information.

2. The method of claim 1 further comprises acknowledging receipt of the indication of the updated public key certificate.

3. The method of claim 1 further comprises providing the public key certificate update subscription information to include identity of at least one subscriber subject and a public key of the at least one subscriber subject.

4. The method of claim 1 further comprises providing the public key certificate update subscription information to include at least one of: signature public key certificate

of at least one subscriber subject and an encryption public key certificate of the at least one subscriber subject.

5. The method of claim 1 further comprises, within step (d), receiving, as the indication of the newly updated public key certificate, at least one of: a new public key certificate for a subscriber subject, a revocation of a public key certificate of the subscriber subject, a change to the public key certificate of the subscriber subject. (encryption or signature certificate)

6. The method of claim 1 further comprises, within step (b), providing the indication of the local replica as at least one of: a copy of the current public key certificate and a message indicating the current public key certificate .

7. The method of claim 1 further comprises, within step (c), receiving the updated public key certificate as at least one of: updates to the current public key certificate and a message regarding updates to the current public key certificate.

8. A method for providing public key certificate updates, the method comprises the steps of:

a) from time to time, receiving a public key certificate update subscription information from a user, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one subscriber subject;

b) monitoring public key certificate of the at least one subscriber subject; and

c) when a change occurs to the public key certificate, providing an indication of the change to the user.

9. The method of claim 8 further comprises:

receiving an indication of a user replica of the public key certificate from the user, when the user is on-line;

determining whether the user replica of the public key certificate is consistent with server replica of the public key certificate; and

when the user replica of the public key certificate is inconsistent with the server replica of the public key certificate, providing an indication of the server replica of the public key certificate to the user.

10. The method of claim 9 further comprises providing the indication as at least one of: the server replica of the current public key certificate and an encoded message identifying differences between the user replica of the public key certificate and the server replica of the public key certificate.

11. The method of claim 8 further comprises, within step (c), providing the indication as at least one of: an encoded message identifying the change to the public key certificate of the at least one subscriber subject.

12. The method of claim 8 further comprises, within step (b), monitoring the public key certificate by pulling the public key certificate of the at least one subscriber subject from a certification authority.

13. The method of claim 8 further comprises receiving information to change the public key certificate of the at least one subscriber subject.

14. The method of claim 8 further comprises, within step (a) receiving from an end-user or system administrator the public key certificate update subscription information.

15. A method for obtaining public key certificate updates, the method comprising the steps of:

a) from time to time, providing, by a user, public key certificate update subscription information to a server, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one subscriber subject;

b) monitoring, by the server, public key certificate of the at least one subscriber subject;

c) when a change occurs to the public key certificate, providing, by the server, an indication of the change to the user;

d) while on-line, receiving, by the user, the indication of the change; and

e) determining, by the user, newly updated public key certificate based on the indication of the change.

16. The method of claim 15 further comprises:

providing, by the user, an indication of a local replica of public key certificate to the server while on-line with the server;

determining, by the server, whether the local replica of the public key certificate is consistent with current public key certificate of the at least one subscriber subject; and

when the local replica of the public key certificate is inconsistent with the current public key certificate, providing, by the server, an indication of a difference between the local replica of the public key certificate and the current public key certificate.

17. A user of secure communication system, wherein the user comprises:

processing unit; and

memory operably coupled to the processing unit, wherein the memory stores programming instructions that, when read by the processing unit, causes the processing unit to (a) from time to time, provide public key certificate update subscription information to a server; (b) provide an indication of a local replica of current public key certificate to the server while on-line with the server; (c) receive updated public key certificate from the serve when the updated public key certificate is inconsistent with the local replica of the current public key certificate; and (d) while on-line, receive newly updated public key certificate from the server, wherein the newly updated public key certificate relates to information of interest as identified in the public key certificate update subscription information.

18. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to acknowledge receipt of the indication of the updated public key certificate.

19. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the public key certificate update subscription information to include identity of at least one subscriber subject and a public key of the at least one subscriber subject.

20. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the public key certificate update subscription information to include at least one of: signature public key certificate of at least one subscriber subject and an encryption public key certificate of the at least one subscriber subject.

21. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to receive, as the indication of the newly updated public key certificate, at least one of: a new public key certificate for a subscriber subject, a revocation of a public key certificate of the subscriber subject, a change to the public key certificate of the subscriber subject.

22. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the indication of the local replica as at least one of: a copy of the current public key certificate and a message indicating the current public key certificate .

23. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to receive the updated public key certificate as at least one of: updates to the current public key certificate and a message regarding updates to the current public key certificate.

24. A server of secure communication system, wherein the server comprises:

processing unit; and

memory operably coupled to the processing unit, wherein the memory stores programming instructions that, when read by the processing unit, causes the processing unit to (a) from time to time, receive a public key certificate update subscription information from a user, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one subscriber subject; (b) monitor public key certificate of the at least one subscriber subject; and (c) provide an indication of a change to the user when the change occurs to the public key certificate.

25. The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to (i) receive an indication of a user replica of the public key certificate from the user, when the user is on-line; (ii) determine whether the user replica of the public key certificate is consistent with server replica of the public key certificate; and (iii) provide an indication of the server replica of the public key certificate to the user when the user replica of the public key certificate is inconsistent with the server replica of the public key certificate.

26. The server of claim 25 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the indication as at least one of: the server replica of the current public key certificate and an encoded message identifying differences between the user replica of the public key certificate and the server replica of the public key certificate.

27. The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide

the indication as at least one of: an encoded message identifying the change to the public key certificate of the at least one subscriber subject.

28. The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to monitor the public key certificate by pulling the public key certificate of the at least one subscriber subject from a certification authority.

29. The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to receive information to change the public key certificate of the at least one subscriber subject.

30. The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to receive from an end-user or system administrator the public key certificate update subscription information.